IN THE CLAIMS

1.-18. (Canceled)

19. (Previously Presented) A method of using an activatable document with an at least machine-readable document number, an optical marking with a machine-readable identification and a storage field disposed on a substrate for receiving an at least machine-readable check number, wherein

to complete the document to provide an authenticity certificate the check number is produced as the result of a cryptographic operation with at least two parameters, the document number and the identification, wherein the identification is optically read out of optical-diffraction structures of the optical marking, and a first secret key, only when the document is put into circulation, and is written into the storage field, and

that after the document is put into circulation the authenticity of the authenticity certificate is checked by means of the check number read out of the storage field and at least the parameters read on the authenticity certificate of the cryptographic operation by means of a second key different from the first key.

20. (Canceled) The method as set forth in claim 19, wherein the machine-readable identification is optically read out of optical-diffraction structures of the optical marking.

21. (Previously Presented) The method as set forth in claim 19, wherein an at least

visually readable, individual code related to a person is written into a check field on the substrate.

22. (Previously Presented) The method as set forth in claim 19, wherein for activation of the document the check number is written in at least machine-readable characters into the storage field arranged on the substrate.

23. (Previously Presented) The method as set forth in claim 19, wherein the check number is written into the storage field of a memory of a microchip located in the substrate and that after the activation procedure the storage field is so blocked that the content of the storage field, once written in, can no longer be altered electronically.

24. (Previously Presented) The method as set forth in claim 19, wherein the magnetically readable check number is written in a magnetic strip arranged on the substrate with the storage field.

25. (Previously Presented) The method as set forth in claim 19, wherein the check number is written at least into a part of the storage field of an optical information carrier arranged on the substrate and that after the activation procedure the check number is optically read out of the optical information carrier which can no longer be altered in the storage field.

26. (Previously Presented) The method as set forth in claim 25, wherein the

identification is written into another part of the optical information carrier.

27. (Previously Presented) A system for activatable documents comprising:

a document, wherein arranged on a substrate of the document is an at least machine-readable document number, an optical marking with a machine-readable identification, wherein the identification is optically read out of optical-diffraction structures of the optical marking, and a storage field for receiving an at least machine-readable check number,

a validation device comprising a transport device for receiving the document without a check number, a computing unit with an input keyboard, a recording means and an optical reader for mechanically reading off the identification, wherein the recording means, the input keyboard and the optical reader are connected to the computing unit, the computing unit is programmed for cryptographic operations with a first secret key for producing the check number by encryption of at least two parameters, the document number and the identification which is read off by the optical reader, and the recording means writes the produced check number into the storage field so that upon being put into circulation the document is completed with the check number to provide an authenticity certificate, and

a verifier comprising a computing unit which provides cryptographic operations with a second key, the optical reader for machine reading of the identification and a receiving means for aligning the authenticity certificate to be checked in the machine reading operation, wherein the computing unit is connected at least to the input keyboard, to a display and to reading-off means and provides the authenticity checking operation by means of the cryptographic operation with

the second key to check the relatedness at least of the numbers recorded on the authenticity certificate, the check number and the parameters used for producing the check number, and which has the display for representing the result of the authenticity check and/or a signal line for the delivery of a permission signal.

28. (Previously Presented) The system for activatable documents as set forth in claim 27, wherein the verifier has an input keyboard for manual input of a personal identification number (PIN) for enablement of the verifier and that the verifier checks the personal identification number of the user.

29. (Previously Presented) The system for activatable documents as set forth in claim 27, wherein the verifier has an input keyboard connected to the computing unit for manual input of the parameters for the cryptographic operation to the computing unit, wherein the parameters include at least the document number and the check number.

30. (Previously Presented) The system for activatable documents as set forth in claim 27, wherein the verifier has at least one reading unit connected to the computing unit for manual input of the parameters for the cryptographic operation to the computing unit, wherein the parameters include at least the document number and the check number.

31. (Previously Presented) The system for activatable documents as set forth in claim

27, wherein the validation device has an input keyboard connected to the computing unit for manual input at least of the document number to the computing unit.

32. (Previously Presented) The system for activatable documents as set forth in claim 27, wherein the validation device has a reading unit connected to the computing unit for manual input of the document number to the computing unit.

33. (Previously Presented) The system for activatable documents as set forth in claim 27, wherein the validation device receives the input of an individual code related to a person, by means of the input keyboard, that the validation device includes a recording means in the validation device for writing the code into the check field, and that the code is one of the parameters for producing the check number in the validation device or for the authenticity check in the verifier.

34. (Previously Presented) The system for activatable documents as set forth in claim 27, wherein the computing unit in the validation device is such that upon encryption of the check number a personal identification number of an authorized person which is inputted by way of an input keyboard is incorporated as a parameter for production of the check number and that the verifier produces the permission signal in the computing unit only when in the authenticity checking procedure the personal identification number is incorporated by way of the input keyboard of the verifier in the computing unit as a parameter of the cryptographic operation.

35. (Previously Presented) The system for activatable documents as set forth in claim 27, wherein at least one validation device and at least one verifier are connected by way of a network to a central computer for bidirectional data exchange.

36. (Previously Presented) The system for activatable documents as set forth in claim 27, wherein the at least one verifier is connected by way of a signal line to a service apparatus and that the service apparatus enables a service by means of the permission signal sent to the service apparatus by way of the signal line.